Claims

What is claimed is:

[c1] A system for secure transfer of wireless data, comprising:

a wireless client;

an enterprise server;

a server stack providing communication services between the enterprise server and the wireless client, wherein the server stack is located on the enterprise server;

a client stack providing communication services between the enterprise server and the wireless client, wherein the client stack is located on the wireless client;

a server-side application adapter providing an interface between the server stack and a server application located on the enterprise server;

a client-side application adapter providing an interface between the client stack and a client application located on the wireless client;

a volatile memory for storing authentication information on the wireless client; and

an authentication manager module managing authentication information in the volatile memory and transferring authentication information to the client-side application adapter.

[c2] The system of claim 1, further comprising:

a wireless gateway providing an interface between the enterprise server and the wireless client.

[c3] The system of claim 1, wherein data transferred between the wireless client and the enterprise server is encrypted.

[c4] The system of claim 3, wherein data is encrypted using Wireless Transport Layer Security protocol embedded within the client stack.

[c5] The system of claim 3, wherein data is encrypted using a Public Key Infrastructure mechanism embedded between the client stack and the client-side application adapter.

[c6] The system of claim 3, wherein data is encrypted using Wireless Transport Layer Security protocol embedded within the client stack and data is encrypted using a Public Key Infrastructure mechanism embedded between the client stack and the client-side application adapter.

[c7] The system of claim 1, wherein the server stack is Wireless Application Protocol compliant.

[c8] The system of claim 1, wherein the client stack is Wireless Application Protocol compliant.

[c9] The system of claim 1, wherein the volatile memory is Random Access Memory.

[c10] The system of claim 1, wherein the client-side application adapter is configured using a configuration file.

[c11] The system of claim 1, wherein the authentication manager module is integrated with the client stack.

[c12] The system of claim 1, wherein the authentication manager module controls a time limit of volatile memory.

[c13] The system of claim 12, wherein the time limit is configurable from within the authentication manager module.

Docket #09649-013001

[c14] The system of claim 12, wherein the volatile memory is erased when the time limit is reached.

[c15] The system of claim 12, wherein the time limit is remotely configurable.

[c16] A system to securely transfer wireless data, comprising:

a wireless client;

an enterprise server;

a server stack providing communication services between the enterprise server and the wireless client, wherein the server stack is located on the enterprise server;

a client stack providing communication services between the enterprise server and the wireless client, wherein the client stack is located on the wireless client;

a server-side application adapter providing an interface between the server stack and a server application located on the enterprise server;

a client-side application adapter providing an interface between the client stack and a client application located on the wireless client;

a volatile memory for storing authentication information on the wireless client;

an authentication manager module managing authentication information in the volatile memory and transferring authentication information to the client-side application adapter; and

a wireless gateway providing an interface between the enterprise server and the wireless client.

[c17] An enterprise server for securely transferring wireless data, comprising:

a server stack providing communication services between the enterprise server and a wireless client, wherein the server stack is located on the enterprise server; and

Docket No. 09649/013001

a server-side application adapter providing an interface between the server stack and a server application located on the enterprise server.

[c18] The enterprise server of claim 17, wherein the server stack is Wireless Application Protocol compliant.

[c19] The enterprise server of claim 17, wherein the server-side application adapter embeds specific business logic into the enterprise server and monitors server applications.

[c20] A wireless client for securely transferring wireless data, comprising:

a client stack providing communication services between an enterprise server and the wireless client, wherein the client stack is located on the wireless client;

a client-side application adapter providing an interface between the client stack and a client application located on the wireless client;

a volatile memory for storing authentication information on the wireless client; and

an authentication manager module managing authentication information in the volatile memory and transferring authentication information to the client-side application adapter.

[c21] The wireless client of claim 20, wherein the client stack is Wireless Application Protocol compliant.

[c22] The wireless client of claim 20, wherein the volatile memory is Random Access Memory.

[c23] The wireless client of claim 20, wherein the authentication manager module integrated with the client stack.

Patent-09649-013001

[c24] The wireless client of claim 20, wherein the authentication manager module controls a time limit of volatile memory.

[c25] The wireless client of claim 24, wherein the time limit is configurable from within the authentication manager module.

[c26] The wireless client of claim 24, wherein the volatile memory is erased when the time limit is reached.

[c27] The wireless client of claim 24, wherein the time limit is remotely configurable.

[c28] The wireless client of claim 20, wherein the client-side application adapter embeds specific business logic into the wireless client and monitors client applications.

[c29] The wireless client of claim 20, wherein the client-side application adapter is configured using a configuration file.

[c30] A method for secure transfer of wireless data from an enterprise server to a wireless client, comprising:
receiving data on the enterprise server;
triggering an event in a server-side application adapter;
forwarding a notification message to a server stack;
sending the notification message from the server stack within the enterprise server to a client stack within the wireless client;
receiving the notification message on the client stack;
forwarding the notification message to a client-side application adapter;
requesting authentication information from an authentication manager module;
checking for authentication information in a volatile memory within the wireless client;
sending a request from the client stack to the enterprise server;
authenticating authentication information on the enterprise server;

opening a secure session between the wireless client and the enterprise server;

transferring data from the server stack to the client stack;

forwarding data to the client-side application adapter; and

forwarding data to a client application.

[c31] The method of claim 30, further comprising:

encrypting data transferred between the wireless client and the enterprise server.

[c32] The method of claim 31, wherein data is encrypted using Wireless Transport Layer Security protocol embedded within the client stack.

[c33] The method of claim 31, wherein data is encrypted using a Public Key Infrastructure mechanism embedded between the client stack and the client-side application adapter.

[c34] The method of claim 31, wherein data is encrypted using Wireless Transport Layer Security protocol embedded within the client stack and data is encrypted using a Public Key Infrastructure mechanism embedded between the client stack and the client-side application adapter.

[c35] The method of claim 30, further comprising:

transferring data between the enterprise server and the wireless client through a wireless gateway, wherein the wireless gateway provides an interface between the enterprise server and the wireless client

[c36] The method of claim 30, further comprising:

controlling a time limit of the volatile memory using the authentication manager module.

[c37] The method of claim 36, wherein the time limit is configurable from within the authentication manager module.

[c38] The method of claim 36, further comprising:
erasing the volatile memory when the time limit is reached.

[c39] The method of claim 36, wherein the time limit is remotely configurable from within the authentication manager module.

[c40] The method of claim 30, further comprising:
configuring the client-side application adapter using a configuration file.

[c41] The method of claim 30, wherein the authentication information comprises a username and a password.

[c42] The method of claim 30, wherein the authentication information comprises a wireless client address and a password.

[c43] The method of claim 30, wherein the volatile memory is Random Access Memory.

[c44] A method for securely transferring wireless data from an enterprise server to a wireless client, comprising:
receiving data on the enterprise server;
triggering an event in a server-side application adapter;
forwarding a notification message to the server stack;
sending the notification message from the server stack within the enterprise server to the client stack within the wireless client;
receiving the notification message on the client stack;
forwarding the notification message to a client-side application adapter;
requesting authentication information from an authentication manager module;
checking for authentication information in a virtual memory within the wireless client;
sending a request from the client stack to the enterprise server;
authenticating authentication information on the enterprise server;

opening a secure session between the wireless client and the enterprise server;

transferring data from the server stack to the client stack;

forwarding data to client-side application adapter;

forwarding data to a client application;

encrypting data transferred between the wireless client and the enterprise server;

transferring data between the enterprise server and the wireless client through a wireless gateway, wherein the wireless gateway provides an interface between the enterprise server and the wireless client;

controlling a time limit of the virtual memory using the authentication manager module;

erasing the volatile memory when the time limit is reached; and

configuring the client-side application adapter using a configuration file.

[c45] A method for securely transferring wireless data from a wireless client to an enterprise server, comprising:

creating data on the wireless client;

forwarding data to a client stack;

forwarding data to a client-side application adapter;

requesting authentication information from an authentication manager module;

checking for authentication information in a volatile memory within the wireless client;

sending a request from the client stack to the enterprise server;

authenticating authentication information on the enterprise server;

opening a secure session between the wireless client and the enterprise server;

transferring data from the client stack to a server stack;

forwarding data to a server-side application adapter; and

forwarding data to a server application.

[c46] The method of claim 45, further comprising:

encrypting data transferred between the wireless client and the enterprise server.

[c47] The method of claim 46, wherein data is encrypted using Wireless Transport Layer Security protocol embedded within the client stack.

[c48] The method of claim 46, wherein data is encrypted using a Public Key Infrastructure mechanism embedded between the client stack and the client-side application adapter.

[c49] The method of claim 45, wherein data is encrypted using Wireless Transport Layer Security protocol embedded within the client stack and data is encrypted using a Public Key Infrastructure mechanism embedded between the client stack and the client-side application adapter.

[c50] The method of claim 45, further comprising:

transferring data between the enterprise server and the wireless client through a wireless gateway, wherein the wireless gateway provides an interface between the enterprise server and the wireless client.

[c51] The method of claim 45, further comprising:

controlling a time limit of the volatile memory using the authentication manager module.

[c52] The method of claim 51, wherein the time limit is configurable from within the authentication manager module.

[c53] The method of claim 51, further comprising:

erasing the volatile memory when the time limit is reached.

[c54] The method of claim 51, wherein the time limit is remotely configurable from within the authentication manager module.

[c55] The method of claim 45, further comprising:

configuring the client-side application adapter using a configuration file.

[c56] The method of claim 45, wherein authentication information comprises a username and a password.

[c57] The method of claim 45, wherein authentication information comprises a wireless client address and a password.

[c58] The method of claim 45, wherein the volatile memory is Random Access Memory.

[c59] A method for securely transferring wireless data from a wireless client to an enterprise server comprising:

creating data on the wireless client;

forwarding data to the client stack;

forwarding data to a client-side application adapter;

requesting authentication information from an authentication manager module;

checking for authentication information in a volatile memory within the wireless client;

sending a request from the client stack to the enterprise server;

authenticating authentication information on the enterprise server;

opening a secure session between the wireless client and the enterprise server;

transferring data from the client stack to the server stack;

forwarding data to the server-side application adapter;

forwarding data to a server application;

encrypting data transferred between the wireless client and the enterprise server;

transferring data between the enterprise server and the wireless client through a wireless gateway, wherein the wireless gateway provides an interface between the enterprise server and the wireless client;

controlling a time limit of the volatile memory using the authentication manager module;

erasing the volatile memory when the time limit is reached; and

configuring the client-side application adapter using a configuration file.

[c60] An apparatus for securely transferring wireless data from an enterprise server to a wireless client, comprising:

means for receiving data on the enterprise server;

means for triggering an event in a server-side application adapter;

means for forwarding a notification message to the server stack;

means for sending a notification message from the server stack within the enterprise server to the client stack within the wireless client;

means for receiving the notification message on the client stack;

means for forwarding the notification message to a client-side application adapter;

means for requesting authentication information from an authentication manager module;

means for checking for authentication information in a volatile memory within the wireless client;

means for sending a request from the client stack to the enterprise server;

means for authenticating authentication information on the enterprise server;

means for opening a secure session between the wireless client and the enterprise server;

means for transferring data from the server stack to the client stack;

means for forwarding data to client-side application adapter; and

means for forwarding data to a client application.

[c61] An apparatus for securely transferring wireless data from a wireless client to an enterprise server, comprising:

means for creating data on the wireless client;

Patent-Pool-09649-013001

means for forwarding data to the client stack;

means for forwarding data to a client-side application adapter;

means for requesting authentication information from an authentication manager module;

means for checking for authentication information in a volatile memory within the wireless client;

means for sending a request from the client stack to the enterprise server;

means for authenticating authentication information on the enterprise server;

means for opening a secure session between the wireless client and the enterprise server;

means for transferring data from the client stack to the server stack;

means for forwarding data to the server-side application adapter; and

means for forwarding data to a server application.

09817470.110501